

JC927 U.S. PRO
10/026535
12/27/01

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: March 26, 2001

Application Number: 2001-087799

Applicant(s): VICTOR COMPANY OF JAPAN, LIMITED

October 26, 2001

Commissioner,
Japan Patent Office

Kozo Oikawa

Number of Certification: 2001-3093625

This Page Blank (uspto)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-261217
 (43)Date of publication of application : 03.10.1997

(51)Int.Cl. H04L 9/10
 G09C 1/00
 G09C 1/00
 H04L 9/30
 H04L 9/32

(21)Application number : 08-072949 (71)Applicant : NIPPON TELEGR & TELEPH CORP
 <NTT>

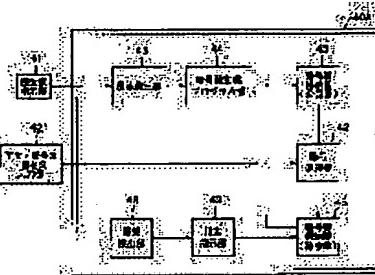
(22)Date of filing : 27.03.1996 (72)Inventor : ISHII SHINJI

(54) COMMUNICATION EQUIPMENT AND ITS METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To generate the key of an open key password without requiring a specified device by providing a means for generating an open key required to inspect a secret key necessary for a signature and the signature inside damper mechanism.

SOLUTION: In a device where ciphered digital data is received, the reception is proved by utilizing the digital signature and ciphered digital data is decoded and processed, a random number generating part 43 and a password key generating program part 44 generate the key of the open key password in accordance with an instruction from a key generation indicating part 41. An open key storing part 45 storing a decoding key for decoding ciphered digital data, a secret key storing part 46 storing a decoding key for decoding ciphered digital data and a password processing part 47 decoding ciphered digital data are arranged inside damper mechanism from which data is not taken out so as to prevent the illegal copying of digital data. The means for generating the necessary open key in order to inspect the secret key required for the signature and the signature is provided inside damper mechanism.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

This Page Blank (uspto)

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-261217

(43)公開日 平成9年(1997)10月3日

(51) Int.Cl. ⁶	識別記号	序内整理番号	F I	技術表示箇所
H 04 L 9/10			H 04 L 9/00	6 2 1 A
G 09 C 1/00	6 2 0	7259-5 J	G 09 C 1/00	6 2 0 B
	6 4 0	7259-5 J		6 4 0 B
H 04 L 9/30			H 04 L 9/00	6 6 3 B
9/32				6 7 5 B

審査請求 未請求 請求項の数 8 OL (全 7 頁)

(21)出願番号 特願平8-72949

(22)出願日 平成8年(1996)3月27日

(71)出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72)発明者 石井 晋司

東京都新宿区西新宿3丁目19番2号 日本
電信電話株式会社内

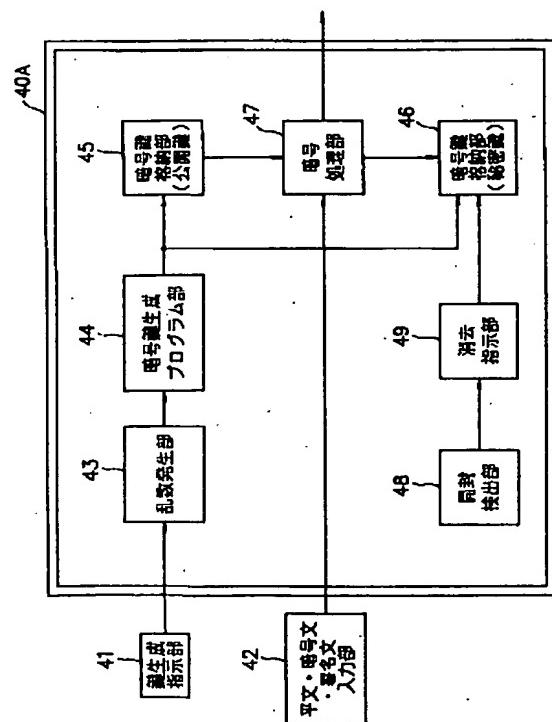
(74)代理人 弁理士 吉田 精孝

(54)【発明の名称】通信装置及びその方法

(57)【要約】

【課題】特別な装置を必要とすることなく公開鍵暗号の鍵を生成し得る通信装置及びその方法を提供すること。

【解決手段】鍵生成指示部41からの指示に従って公開鍵暗号の鍵を生成する乱数発生部43及び暗号鍵生成プログラム部44と、該生成した鍵を格納する暗号鍵格納部45, 46と、平文・暗号文・署名文入力部42から入力される平文または暗号文もしくは署名文を前記鍵を用いて暗号化しました復号もししくは署名する暗号処理部47とを、開封検出部48により開封を検出すると消去指示部49によって暗号鍵格納部46に格納した秘密鍵を消去する個人携帯デバイス40の被い40A内に設けておくことにより、該デバイス40がない限り情報を利用できないようにして不正コピーを防止する。



【特許請求の範囲】

【請求項1】 暗号化されたデジタルデータを受信し、該受信をデジタル署名を利用して証明し、前記暗号化されたデジタルデータを復号して何人にも知られないように処理する装置であって、署名に必要な秘密鍵を記憶する秘密鍵記憶手段と、暗号化されたデジタルデータを復号する復号鍵を記憶する復号鍵記憶手段と、暗号化されたデジタルデータを復号する暗号化データ復号手段とを、データの取り出しが不能なタンパ機構内に配置することによりデジタルデータの不正コピーを防止した通信装置において、

署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成する鍵生成手段をタンパ機構内に設けたことを特徴とする通信装置。

【請求項2】 デジタルデータとして符号化された情報もしくは実行プログラムを用いたことを特徴とする請求項1記載の通信装置。

【請求項3】 タンパ機構に属する手段のうち少なくとも秘密鍵記憶手段と復号鍵記憶手段と鍵生成手段とを、タンパ機能を有しつつ携帯可能で本体に対しデータのやりとりが可能な筐体内に配置したことを特徴とする請求項1または2記載の通信装置。

【請求項4】 情報の発信側と受信側とがネットワークを介して結ばれている状態にて、発信側が発信したデジタルに符号化された情報を受信者が確かに受信したこととを証明することと、符号化されたデジタル情報を復号した状態で利用することはできるが、そのデジタル情報をコピーすることはできないようにするために、発信側の装置は、

符号化されたデジタル情報を暗号化する送信側暗号化手段と、

暗号化したデジタル情報を受信側に送る暗号化データ送信手段とを具備し、
受信側の装置は、

暗号化データを受信する暗号化データ受信手段と、
暗号化されたデジタルデータを復号する暗号化データ復号手段と、

符号化されたデジタルデータを復号する符号化データ復号手段と、

暗号化データ復号手段と符号化データ復号手段とを連結する連結手段と、

連結手段のデジタルデータを何人にも知られないようになるための再生用タンパ機構と、

暗号化データを復号する復号鍵を保持する復号鍵記憶手段と、

暗号化されたデータを受信したことをデジタル署名を利用して証明する署名手段と、

署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成する鍵生成手段と、

署名に必要な秘密鍵を記憶する秘密鍵記憶手段と、

署名の検証に必要な公開鍵を公開する公開鍵出力手段と、

復号鍵記憶手段、鍵生成手段及び秘密鍵記憶手段の入出力結果を何人にも知られないようにするための鍵用タンパ機構とを具備したことを特徴とする通信装置。

【請求項5】 情報の発信側と受信側とがネットワークを介して結ばれている状態にて、発信側が発信した実行プログラムを受信者が確かに受信したことを証明することと、受信した実行プログラムを実行することはできるが、プログラムをコピーすることはできないようにするために、

発信側の装置は、

実行プログラムを暗号化する送信側暗号化手段と、
暗号化した実行プログラムを受信側に送る暗号化データ送信手段とを具備し、
受信側の装置は、

暗号化データを受信する暗号化データ受信手段と、
暗号化された実行プログラムを復号する暗号化実行プログラム復号手段と、

実行プログラムを実行するプログラム実行手段と、
暗号化実行プログラム復号手段とプログラム実行手段とを連結する連結手段と、
連結手段の復号後のデジタルデータを何人にも知られないようにするためのプログラム実行用タンパ機構と、暗号化データを復号する復号鍵を保持する復号鍵記憶手段と、

暗号化されたデータを受信したことをデジタル署名を利用して証明する署名手段と、

署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成する鍵生成手段と、

署名に必要な秘密鍵を記憶する秘密鍵記憶手段と、
署名の検証に必要な公開鍵を公開する公開鍵出力手段と、

復号鍵記憶手段、鍵生成手段及び秘密鍵記憶手段の入出力結果を何人にも知られないようにするための鍵用タンパ機構とを具備したことを特徴とする通信装置。

【請求項6】 鍵用タンパ機構に属する手段を備えた携帯可能な筐体と、鍵用タンパ機構に属する手段を除いた受信側の装置とを具備し、前記筐体と受信側の装置とのそれぞれにデータのやりとりを行うインターフェース手段を設けたことを特徴とする請求項4または5記載の通信装置。

【請求項7】 情報の発信側と受信側とがネットワークを介して結ばれている状態にて、発信側が発信したデジタルに符号化された情報を受信者が確かに受信したことを証明することと、符号化されたデジタル情報を復号した状態で利用することはできるが、そのデジタル情報をコピーすることはできないようにするために、
送信側では、
符号化されたデジタル情報を暗号化し、

該暗号化したデジタル情報を受信側に送り、
受信側では、
ネットワークを介して暗号化データを受信し、
暗号化の復号と符号化の復号を行う部分のデジタルデータを何人にも知られないようにし、
暗号化データを復号する鍵を保持し、
暗号化されたデータを受信したことをデジタル署名を利用して証明し、
デジタル署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成し、
署名に必要な秘密鍵を記憶し、
署名の検証に必要な公開鍵を公開し、
暗号化されたデジタルデータを復号し、
符号化されたデジタルデータを復号し、
デジタルデータの復号鍵、署名用の鍵生成及び署名用の秘密鍵の入出力結果を何人にも知られないようにすることを特徴とする通信方法。

【請求項8】 情報の発信側と受信側とがネットワークを介して結ばれている状態にて、発信側が発信した実行プログラムを受信者が確かに受信したことを証明することと、発信側の手順として実行プログラムを復号した状態で利用することはできるが、その実行プログラムをコピーすることはできないようにするために、
送信側では、
実行プログラムを暗号化し、
暗号化した実行プログラムを受信側に送り、
受信側では、
ネットワークを介して暗号化データを受信し、
暗号化の復号と実行プログラムを実行する部分のデジタルデータを何人にも知られないようにし、
暗号化データを復号する鍵を保持し、
暗号化されたデータを受信したことをデジタル署名を利用して証明し、
デジタル署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成し、
署名に必要な秘密鍵を記憶し、
署名の検証に必要な公開鍵を公開し、
暗号化された実行プログラムを復号し、
必要ならば実行プログラムを実行し、
デジタルデータの復号鍵、署名用の鍵生成及び署名用の秘密鍵の入出力結果を何人にも知られないないようにすることを特徴とする通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、特別な装置を必要とすることなく公開鍵暗号の鍵を生成し得る通信装置及びその方法に関するものである。

【0002】

【従来の技術】音声・映像情報や実行プログラムのような著作権を有するデジタルデータを、ネットワークを

利用して販売しようとする場合、利用者認証及び配送確認とともに不正コピーの防止が問題となる。

【0003】利用者認証を解決する方法としては、デジタル暗号アルゴリズムの公開鍵暗号を利用する方法がある。以下、公開鍵暗号について簡単にふれておく。

【0004】デジタル暗号アルゴリズムには、共通鍵暗号アルゴリズム（秘密鍵暗号アルゴリズム）と公開鍵暗号アルゴリズムとがある。

【0005】共通鍵暗号アルゴリズムは、高速演算が可能であるが、暗号化鍵と復号鍵に同じ共通鍵を使用することから、通信する両者のみがその共通鍵を秘密に保持する必要がある。一方、公開鍵暗号アルゴリズムは、共通鍵暗号アルゴリズムに比べて計算量が多く、高速処理には向きであるが、暗号化鍵と復号鍵に異なる鍵を使用するため、暗号化鍵を公開しておくことにより、共通鍵暗号アルゴリズムの共通鍵のように鍵を秘密に配達する必要がなくなる。

【0006】ところが、公開鍵暗号アルゴリズムでは、暗号化鍵を公開していることから誰もが暗号文を作成することができる。このため、暗号化されて送られてきた通信文等を、誰が暗号化して送ってきたかを証明することも必要になる。そこで、考えられるようになったのが署名を利用した相手認証である。

【0007】相手認証機能を備えた公開鍵暗号アルゴリズムの代表例として、RSA暗号がある。これは暗号通信に関して、暗号化する時には暗号化鍵を利用し、復号する時には復号鍵を利用し、また、署名を生成する時は復号鍵を利用し、その署名を検証する時は暗号化鍵を利用するものである。

【0008】一方、配達すべきデジタルデータを暗号化するには、公開鍵暗号ではなく共通鍵暗号が使われることがほとんどである。その最大の理由は、非常に大きなデジタルデータの暗号処理には、公開鍵暗号に比べて極めて高速な共通鍵暗号の方が適しているからである。

【0009】

【発明が解決しようとする課題】しかし、共通鍵暗号アルゴリズムでは、通信する両者が共通の秘密鍵を所有していないなければならない。そこで、共通鍵暗号に使う共通の秘密鍵を公開鍵暗号を利用して相手を認証し、配達することが一般的である。しかし、それだけでは利用者のコピーは防ぐことはできない。そこで、利用者認証に用いる秘密鍵を、タンパ機構（装置）を用いることにより誰にも知られることのないようにして、個人携帯デバイスを作成できることを特徴とした発明（特願平7-155030号、特願平7-159414号、特願平7-204642号）を提案した。しかし、これらの発明では、個人携帯デバイスにユーザの秘密鍵を埋め込むためのタンパ装置が必要になるという問題があった。

【0010】本発明の目的は、特別な装置を必要とする

ことなく公開鍵暗号の鍵を生成し得る通信装置及びその方法を提供することにある。

【0011】

【課題を解決するための手段】本発明では、前記課題を解決するため、暗号化されたディジタルデータを受信し、該受信をデジタル署名を利用して証明し、前記暗号化されたディジタルデータを復号して何人にも知られないように処理する装置であって、署名に必要な秘密鍵を記憶する秘密鍵記憶手段と、暗号化されたディジタルデータを復号する復号鍵を記憶する復号鍵記憶手段と、暗号化されたディジタルデータを復号する暗号化データ復号手段と、データの取り出しが不能なタンパ機構内に配置することによりディジタルデータの不正コピーを防止した通信装置において、署名に必要な秘密鍵及び署名を検証するために必要な公開鍵を生成する鍵生成手段をタンパ機構内に設けた。

【0012】ネットワークを利用したデジタル情報販売システムでは、本人を含めて誰もが知らない本人の秘密鍵と、本人しか所有していない秘密鍵を特別な専用装置なしに生成することができることから、・本人の確認のために相手認証機能を行える、・デジタル著作権情報を購入した本人でさえ、不正コピーをすることができないシステムを提供することができる。

【0013】

【発明の実施の形態】以下、図面に従って本発明の実施の形態を説明するが、ここでは公開鍵暗号アルゴリズムの中で暗号機能と認証機能を合わせ持ち、最も広く利用されているRSA暗号を用いて説明する。なお、RSA暗号の詳細については、池野、小山共著「社団法人電子情報通信学会編『現代暗号理論』」の「第6章 RSA公開鍵暗号」に詳述されている。

【0014】(第1の形態) 図1は本発明を利用してサービスを行うシステム全体の基本的な構成を示すもので、図中、10はコンテンツサーバ、20はネットワーク、30は個人用端末、40は個人携帯デバイスである。

【0015】コンテンツサーバ10はサービスを提供する。サービスを利用する者が、個人用端末30に個人携帯デバイス40を差し込み、該個人用端末30を操作することにより、コンテンツサーバ10からネットワーク20を介して個人用端末30にコンテンツを配布させる。

【0016】図2は個人携帯デバイス40の詳細を示すもので、図中、41は鍵生成指示部、42は平文・暗号文・署名文入力部、43は乱数発生部、44は暗号鍵生成プログラム部、45、46は暗号鍵格納部、47は暗号処理部、48は開封検出部、49は消去指示部である。

【0017】前記構成中、鍵生成指示部41及び平文・暗号文・署名文入力部42を除く部分は、いかなる者も

その内部に触れることができない被い(タンパ機構)40Aの中である。例え、この個人携帯デバイス40の所有者であっても被い40Aを無理に開けて、内部に保存されているRSA暗号の秘密鍵を読み出そうとすると、開封検出部48が開封を検出し、消去指示部49により内部の秘密情報を電気的に消去する。また、違う鍵に書き換えたりすることもできないように、開封すると個人携帯デバイス40の内部で使用している半導体チップの端子や基盤の配線も壊れるように製造してある。

【0018】個人携帯デバイス40は、2つの入力系と1つの出力系を備えている。入力系のうちの1つはRSA暗号の鍵生成指示部41である。これは、ユーザがこの個人携帯デバイス40を利用してサービスを受けようとする前に、今後、使用するRSA暗号の公開鍵と秘密鍵を生成する指示である。鍵生成指示部41によって指示される具体的な例は、乱数発生部43で使用する乱数のシード(種)である。

【0019】ここで使用するシードはほぼ2度と同じシードを発生することのない方法がふさわしい。例え、キーボード入力の入力文字とその入力時間間隔を利用するのが実用的である。入力されたシードは、乱数発生部43で乱数となり、暗号鍵生成プログラム部44に与えられる。暗号鍵生成プログラム部44はRSA暗号の鍵を生成する。暗号鍵生成プログラム部44で生成されたRSA暗号の鍵のうち、公開鍵は公開する必要があるので、個人携帯デバイス40の外部から読み出しが可能な公開鍵格納部45に格納される。一方、秘密鍵の方は読み出すことができないように秘密鍵格納部46に格納される。

【0020】以上で個人携帯デバイス40の内部で使用する鍵の準備は終了である。

【0021】サービスを受ける場合、平文の暗号化/暗号文の復号、署名/検証が必要になったときにバラメータがもう1つの入力系、つまり平文・暗号文・署名文入力部42に入力される。入力された平文の暗号化及び署名文の検証には、相手の公開する公開鍵を使用する。暗号文の検証には、秘密鍵格納部46の秘密鍵を利用して、暗号処理部47にて演算し出力される。

【0022】このようにして生成したRSA暗号の秘密鍵は、個人携帯デバイス40を所有するものだけが使用できることを誰にでも納得させることができ、かつ秘密鍵の値そのものは個人携帯デバイス40を所有するものも含めて誰も知ることができないことを誰もが納得することができる。

【0023】言い換えると本発明の課題であった、・本人の確認のために相手認証機能を行える、・デジタル著作権情報を購入した本人でさえ、不正コピーをすることができないシステムを提供することができ、しかも、個人携帯デバイス40で使用する秘密鍵を特別な装置なしに実現することができる。

【0024】個人携帯デバイス40の実際の例としては、規格化されているICカード、PCカード（PCM CIA）を用いて容易に実現できる。

【0025】また、受信側で実際に復号したコンテンツを利用する方法としては、特願平6-298702号、特願平6-299940号で提案したものがある。

【0026】なお、鍵生成指示部41及び平文・暗号文・署名文入力部42は本デバイス40を差し込む個人用端末30側に設けても良く、また、個人用端末30と個人携帯デバイス40とを一体化することもできる。

【0027】図3は個人情報デバイスにおける鍵生成手順を示すフローチャートである。

【0028】最初に、個人携帯デバイス40の所有者が、鍵生成開始を指示する（s1）。この指示により、個人携帯デバイス40は乱数用シードを作成する（s2）。その後、これをを利用して乱数を生成し（s3）、鍵生成プログラムを起動し（s4）、鍵を生成する。生成した鍵のうち、公開鍵は通信相手に配布する必要があるので、個人携帯デバイス40から出力する（s5）。出力された公開鍵を個人携帯デバイス40の所有者が受け取り（s6）、必要ならば、証明書発行機関などに公開鍵を登録し、承認された後、その公開鍵を通信相手に配布する。

【0029】一方、個人携帯デバイス40は、秘密鍵を個人携帯デバイス40の秘密鍵読み出し不可領域に格納し（s7）、鍵生成を終了する。

【0030】図4は個人情報デバイスにおける鍵消去手順を示すフローチャートである。

【0031】個人携帯デバイス40の所有者を含めた何者かが、個人携帯デバイス40の内部の秘密情報を取り出すために、細工をしようとする場合を想定する。最初は、個人携帯デバイス40と個人用端末30とのインターフェースから何らかの秘密情報が取り出せないかどうか試みると考えられる。しかしながら、当然公開可能な情報以外は出力されないので、秘密情報を得ることはできない。そこで、ここであきらめない場合、個人携帯デバイス40の中を開封し、秘密情報を取り出そうと試みる

と考えられる。

【0032】もし、少しでもデバイスのケースをこじ開けようとする（sp1）と、デバイス開封が検出され（sp2）、秘密鍵消去プログラムが起動されて（sp3）、秘密鍵が消去される（sp4）。

【0033】また、個人携帯デバイス40を無理にこじ開ける（sp5）と、搭載された主なチップが破壊され（sp6）、情報の取り出しが不可能となる。

【0034】このように、たとえ個人携帯デバイス40を開封し、秘密情報を得ようとしても不可能である。

【0035】

【発明の効果】以上説明したように、本発明によれば、個人携帯デバイスを用いて、誰もが知り得ない公開鍵暗号の秘密鍵をユーザのみが使用できる証明をすることができる個人用の秘密鍵を特別な専用装置を用いることなく生成することができる。

【0036】この個人携帯デバイスを使用することにより、特別なネットワーク上でデジタル情報を商品として取り扱う場合に、支払い意志を表明したものはユーザが唯一であることが証明でき、かつユーザがデジタル情報を情報提供者に無断でコピーできないことが証明できるようになる効果がある。

【図面の簡単な説明】

【図1】本発明を利用してサービスを提供するシステム全体の構成図

【図2】個人携帯デバイスの詳細を示す構成図

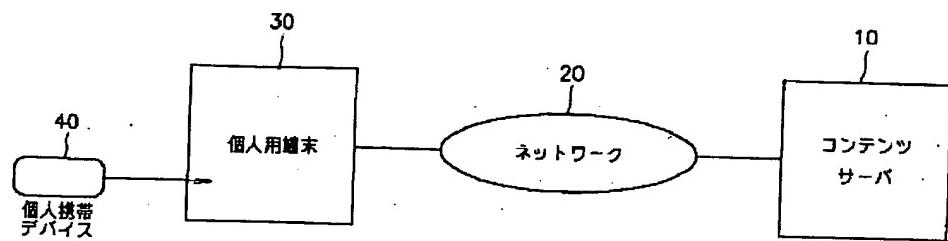
【図3】個人携帯デバイスにおける鍵生成手順を示すフローチャート

【図4】個人携帯デバイスにおける鍵消去手順を示すフローチャート

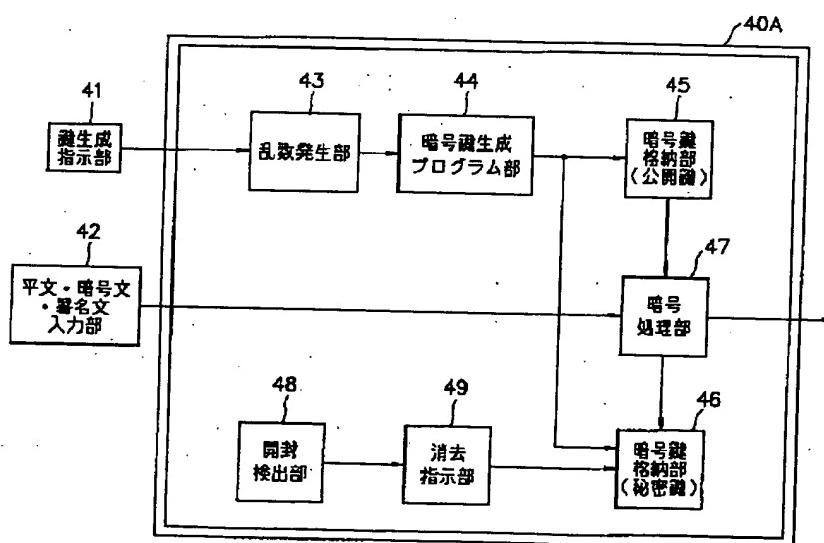
【符号の説明】

10…コンテンツサーバ、20…ネットワーク、30…個人用端末、40…個人携帯デバイス、41…鍵生成指示部、42…平文・暗号文・署名文入力部、43…乱数発生部、44…暗号鍵生成プログラム部、45，46…暗号鍵格納部、47…暗号処理部、48…開封検出部、49…消去指示部、40A…被い。

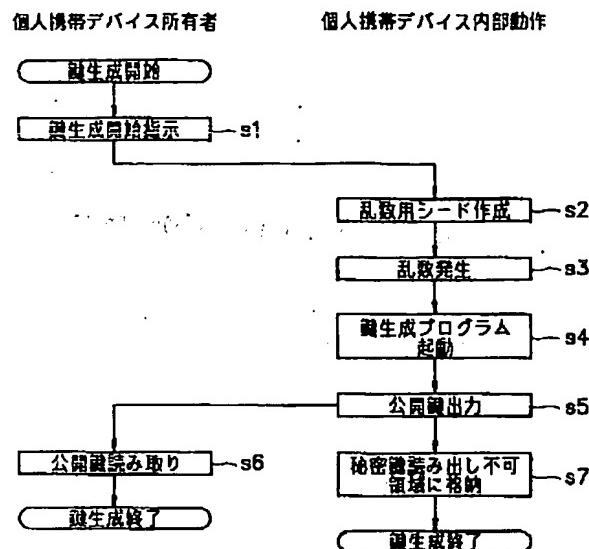
【図1】



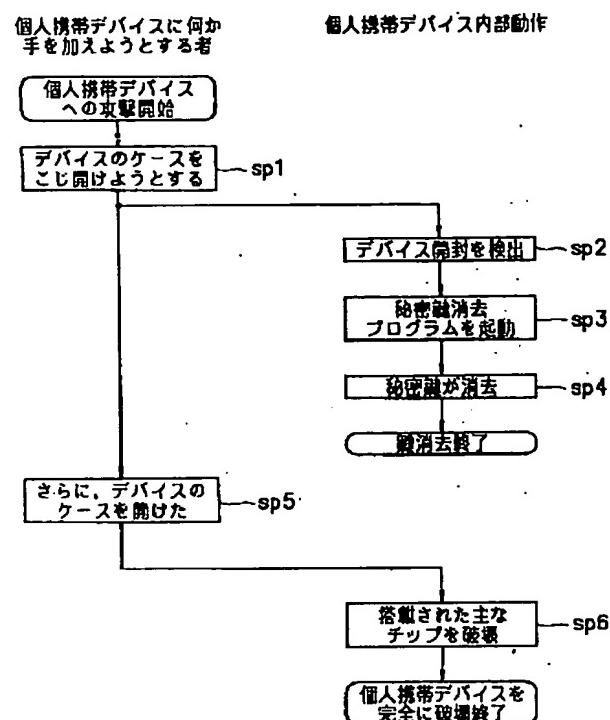
【図2】



【図3】



【図4】



This Page Blank (uspto)